EXHIBIT 3

24

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT
CIVIL ACTION NO.

ATTORNEY GENERAL
MAURA HEALEY,

Petitioner,

v.

FACEBOOK, INC.,

Respondent.

PETITION TO COMPEL COMPLIANCE WITH CIVIL INVESTIGATIVE DEMAND PURSUANT TO G.L. C. 93A, § 7

Pursuant to G.L. c. 93 A, § 7, Attorney General Maura Healey files this Petition to compel compliance with Civil Investigative Demand No. 2018-CPD-67 ("CID"), issued to Respondent Facebook, Inc. ("Facebook"), because Facebook is withholding responsive materials without a valid basis. In support of this Petition, the Attorney General attaches exhibits obtained through her investigation[1] and submits the accompanying Memorandum of Law in Support of the Attorney General's Petition ("Memorandum") and states as follows:

Introduction

1. After learning that a software developer obtained and sold Facebook data for tens of millions of Facebook users without their consent, Facebook conducted an investigation to identify other applications ("apps") that may have engaged in similar misuse of consumer data. Through that investigation, Facebook has identified approximately 10,000 applications that may also have misappropriated and/or misused consumers' personal data from the Facebook Platform. Despite a Civil Investigative Demand ("CID") from the Massachusetts Attorney General's Office for this information, Facebook refuses to disclose the identities of these

[1] An index of exhibits appears at the end of this Petition. In an electronic version of this Petition, provided to the Court and served on Respondent, the cited exhibits are hyperlinked to an electronic copy.

applications and developers. Facebook is withholding this information based on a claim that the information is protected attorney work product. This claim is meritless and the Court should compel Facebook to comply with the Attorney General's CID and disclose all information requested regarding these apps and developers to the Massachusetts Attorney General's Office.

2. News broke in March 2018 that a professor, Alexander Kogan, the developer of a software application called "thisisyourdigitallife" ("Kogan's App"), had obtained sensitive personal data of over 80 million Facebook users using functionalities that Facebook offered developers, and then, in violation of Facebook's data use policies, sold some or all of that data to a third-party political data analytics firm.

3. In response to widespread public outcry, Facebook publicly admitted that this episode may not be an isolated incident, and announced an initiative, which it dubbed the "App Developer Investigation" (or "ADI"), that it claimed was designed to evaluate whether any of the other millions of apps that were on the Facebook Platform at the same time as Kogan's App had likewise obtained and then sold, misappropriated, or otherwise misused Facebook users' data. Facebook has repeatedly touted the ADI to its user base, its investors, the general public, and even Congress as an effective method to uncover data misuse.

4. The Attorney General, pursuant to her authority to investigate unfair or deceptive trade practices, commenced an investigation into Facebook's oversight and monitoring of third-party applications on the Facebook Platform and the misuse of non-public information of Facebook users by third-party application developers or others.

5. As part of that investigation, the Attorney General's Office has issued multiple Civil Investigative Demands under G.L. c. 93A, § 6 to Facebook. In addition to seeking information about Facebook's practices to enforce its various privacy and data use policies

(which purported, among other things, to restrict app developers' collection, use, and disclosure of users' data) and safeguard its users' data, the Attorney General has specifically demanded that Facebook identify any other third parties that may have misappropriated consumers' data from the Facebook Platform or otherwise engaged in conduct that violated Facebook's data use policies or the law. *See* Civil Investigative Demand No. 2018-CPD-67, dated November 5, 2018 (the "CID"), attached hereto as **Exhibit A.**

6. Despite the Attorney General's compelling interest in determining whether other apps or app developers acquired and used consumers' personal data without authorization, and despite that this information is in the sole possession and knowledge of Facebook, Facebook has refused to comply with these certain demands in the CID, or otherwise disclose to the Attorney General pertinent information about the scope of conduct, apps, or app developers that it is purporting to investigate. In so refusing, Facebook has taken the position that the identity of certain apps and app developers who may have misappropriated or misused consumers' data from its Platform, and information relating or emanating from them, is protected from disclosure by the attorney work product doctrine.

7. This petition is required because by refusing to comply, Facebook is preventing the Attorney General from identifying potential violations of law by Facebook and others, and from assessing the full scope of potential harm to Massachusetts consumers.

8. As set forth in more detail in the accompanying Memorandum, Facebook's claims of work product protection are factually unfounded and not supported by applicable law. Furthermore, Facebook has waived its right to seek judicial relief excusing its production, and has no valid basis to refuse to produce this information to the Attorney General. For the reasons

set forth below, and as discussed in greater detail in the accompanying Memorandum, this Court should compel Facebook's production.

The Parties

9. The Attorney General's Office ("AGO") is conducting an investigation pursuant to the Massachusetts Consumer Protection Act, G.L. c. 93A, § 6, into Facebook's oversight and monitoring of third-party applications on the Facebook Platform and the potential misappropriation and misuse of non-public information of Facebook users by third-party application developers or others.

10. Facebook is a Delaware corporation with its headquarters and principal place of business at 1 Hacker Way (1601 Willow Road), Menlo Park, California 94025. Facebook also maintains offices at 100 Binney St., Cambridge, Massachusetts 02142.

11. Facebook offers Massachusetts residents various goods and services, including a social networking website and mobile application, as set forth below.

Facebook and the Facebook Platform

12. Facebook is a social networking website and mobile application that allows consumers ("users") to create personal profiles and connect with other users ("Friends" in Facebook terminology) on mobile devices and personal computers.

13. As of June 2019, Facebook had more than 1.59 billion daily active user accounts and over 2.41 billion monthly active user accounts.

14. Using Facebook's website, mobile application, and associated functionalities, users can (and could, at all relevant times) choose to disclose and share personally-identifying data about themselves with other users of their choosing—including their name, birthdate, gender identity, current city, hometown, occupation, religion, interests, political affiliation, education, and photos or videos of themselves and others. Users also generate other data based

on their activity on Facebook, such as by posting comments on their Facebook profile or that of their Friends, posting and commenting on photos (of themselves, their kids, their friends, etc.), "liking" or "reacting"[2] to comments, photos, or websites, watching videos, or linking to or engaging with other webpages, or by viewing and interacting with the profile pages of their Friends or other entities (such as businesses, brands, or political organizations).

15. Facebook also operates the Facebook "Platform," a technological infrastructure that allows third-party software application developers ("app developers") to run an unlimited number of applications ("apps") that integrate with Facebook and interact with Facebook users Apps can include games, location-based services, music playing services, news or other media services, etc. When users use the apps by logging into Facebook or by installing them, Facebook allows the app and its developer to obtain personal data, including any or all of the data described *supra,* ¶ 14, from their Facebook account using software communication protocols called application programing interfaces, or "APIs."

16. From 2012 to May 1, 2015, Facebook operated "Version 1" of the Platform, which allowed apps to obtain personal data from the Facebook accounts of not only users that installed or engaged directly with an app, but also personal data pulled from the accounts of the user's Facebook Friends who had not installed or engaged directly with the app. A user's Friend could deauthorize this type of sharing by adjusting their Facebook account settings, but for some time, Facebook set users' settings so that this sharing was permitted by default, unless the user affirmatively changed it in their account settings.

[2] A "Reaction" is a button within Facebook that allows users to indicate a reaction to other users' photos, videos, or postings, or for webpages, apps, or advertisements. Originally, Facebook only had one reaction—the "Like" button—but more have developed, including, for example, "Love," "Angry," and "Sad."

17. The ability of an app to obtain highly personal and sensitive data not just from Facebook's users but also their Friends was a core value proposition that Facebook offered app developers during this time. In Facebook's April 23, 2012 Registration Statement for its initial public offering, Facebook touted that the way it enticed developers to the Platform was by enabling them "to easily integrate with Facebook" and thereby "reach [Facebook's] 900 million users," obtain personalized information on those users, and gain new "social distribution channels to increase traffic to" the developers' apps. In turn, Facebook viewed "the success of . . . Platform developers" (app developers), as "key to increasing user engagement" on the Platform, especially as users spent more time using apps on mobile devices. *See* **Exhibit B** at 3-4.

18. In its April 23, 2012 pre-IPO SEC Registration Statement, Facebook stressed this symbiotic relationship with app developers as a critical component of its value:

> User engagement with our Platform developers' apps and websites creates value for Facebook in multiple ways: our Platform supports our advertising business because apps on Facebook create user engagement that enables us to show ads; our Platform developers purchase advertising on Facebook to drive traffic to their apps and websites; Platform developers use our Payment system to facilitate transactions with users; and users' engagement with Platform apps and websites contributes to our understanding of users' interests and preferences, improving our ability to personalize content. We continue to invest in tools and APIs that enhance the ability of Platform developers to deliver products that are more social and personalized and better engage users on Facebook, across the web, and on mobile devices.

Exhibit B at 93.

19. As of March 31, 2012, over nine million apps and websites had integrated with the Facebook Platform to gain access the rich stream of data that over 900 million Facebook users generated. **Exhibit B** at 87.

20. In April 2014, Facebook announced that it was launching "Version 2" of its Platform and going forward, would be restricting the scope of data that an app developer would

be able to access through the Platform. Under "Version 2" of the Platform, app developers could no longer access data about Friends of the installing user, and could obtain only basic information about the installing user (basic profile information, email address, and a list of Friends who also used the app) unless they sought and obtained from Facebook permission to obtain additional data. Facebook allowed apps a grace period of one year, to May 1, 2015, to continue operating on the Version 1 Platform (and to enjoy its expanded data access) before transitioning to Version 2. *See* **Exhibit C**.

Facebook's Promises Regarding the Protection of User Data on the Platform

21. At all relevant times, a variety of policies, terms, and conditions governed the use of Facebook and the Platform by users and developers. These policies included Facebook's "Data Use Policies,"[3] to which all users and developers must consent before using Facebook, its "Statement of Rights and Responsibilities" or "SRR,"[4] which constitutes the terms of service that govern Facebook's relationship with users and others who interact with Facebook, and its "Platform Policy," which sets forth the rules governing app developers' access to and conduct on the Platform (together with the Data Use Policy and the SRR, "Facebook's Policies").

22. At all relevant times, Facebook's Policies contained various promises and representations to users regarding what Facebook purportedly permitted and prohibited app developers from doing vis-a-vis user data, including that Facebook:

- Prohibited app developers from selling or licensing user data obtained from Facebook to any other third party;[5]

[3] Also called the "Data Policy." For ease of reference, all versions will be referred to herein as the "Data Use Policy."
[4] Also called the "Terms of Service." For ease of reference, all versions will be referred to herein as the "SRR" or "Statement of Rights and Responsibilities."
[5] *See* **Exhibit D** (SRR), at sections 9.2.6, 9.2.7 (FB-AG-00000144-145); **Exhibit E** (Platform Policy), at sections II.6, II.9 (FB-AG00000042).

- Prohibited app developers from sharing any user data obtained from Facebook with any ad network, data broker or other advertising service;[6]
- Restricted app developers from requesting data from users that was not necessary for the functioning of the app;[7] and
- Required app developers to "[p]rotect the information you receive from us against unauthorized access or use."[8]

23. Consistent with these various restrictions on app developers' use and disclosure of Facebook users' data, Facebook assured users in 2012 through 2014 (when Version 1 of the Platform allowed an app to obtain data about the installing user and the user's Friends, *see supra,* ¶ 16) that "[i]f an application asks permission from someone else [i.e. the user's Friend] to access your information, the application will be allowed to use that information only in connection with the person that gave the permission, and *no one else*." **Exhibit G** (emphasis added) at FB-AG-00000019; **Exhibit H** (emphasis added) at FB-AG-0000034-35.

24. Facebook also represented to users it would enforce these restrictions against app developers. In its Platform Policy, Facebook warned app developers that it:

> [M]ay enforce against your app or web site if we conclude that your app violates our terms or is negatively impacting the Platform. ... Enforcement is both automated and manual, and can include disabling your app, restricting you and your app's access to platform functionality, requiring that you delete data, terminating our agreements with you or any other action that we deem appropriate.

Exhibit F (Platform Policy) at sections 6.15, 6.16 (FB-AG-00000066); *see also* **Exhibit E** (2013 Platform Policy), section V (similar representations) (FB-AG-00000043).

25. Facebook further warned app developers that it "can audit your app to ensure it is safe and does not violate our Terms. If requested, you must provide us with proof that your app

[6] *See* **Exhibit D** (SRR), at sections 9.2.6, 9.2.7 (FB-AG-00000144-145); **Exhibit E** (Platform Policy), at sections II.6, II.9 (FB-AG00000042).
[7] *See* **Exhibit D** (SRR) at section 9.2.1 (FB-AG-00000144); **Exhibit E** (Platform Policy), at section II.1 (FB-AG00000042).
[8] **Exhibit F** (Platform Policy as of July 24, 2014), at section 3.1 (FB-AG00000063).

complies with our terms." **Exhibit F** (Platform Policy) at section 6.8 (FB-AG-00000066); *see also* **Exhibit D** (SRR) at section 9.2.18 (FB-AG-00000145) ("[t]o ensure your application is safe for users, we can audit it.").

26. Finally, Facebook warned developers that they could be "require[d]" by Facebook "to delete user data if [they] use it in a way that [Facebook] determine[s] is inconsistent with users' expectations." **Exhibit D** (SRR) at section 9.2.8 (FB-AG-00000145).

Facebook's Pre-2018 Practices to Enforce its Policies Against App Developers

27. As of 2012, Facebook "put in place an enforcement program to prevent and respond to potential developer misuse of user information" and "dedicated significant internal and external resources to this program, including for detecting, escalating, investigating, and combating violations of Facebook's policies." **Exhibit I** at Appendix A, p. 1 (FB-CA-MAAG-NYAG-C012.01).[9]

28. This includes an internal "Development Operations" or "DevOps" team, which "has consistently played a central role in enforcing Facebook's policies and protecting user data and Facebook's Platform" by "[redacted]" and using "[redacted]." **Exhibit I** at FB-CA-MAAG-NYAG-C012.06.

29. Facebook also utilized various "[redacted]," as well as "[redacted]

[9] In this and various other exhibits, the AGO has redacted the names and identifying information of certain non-party individuals and/or entities. The AGO can provide unredacted copies of these exhibits at the Court's request.

[redacted]" **Exhibit I** at FB-CA-MAAG-NYAG-C012.06-12.07.

30. Facebook has produced documents to the Attorney General illustrating its policy enforcement practices from 2012 through 2018, such as training documents, enforcement criteria, or specific examples of enforcement. *See, e.g.,* **Exhibit J** (training presentation on app compliance from 2013); **Exhibit K** at FB-CA-MAAG-NYAG-00041068 (showing enforcement against "paid social sharing apps" in 2012).

31. In connection with its efforts to enforce its polices, Facebook utilized various "enforcement rubrics" that identify examples of violations of Facebook policies, designate certain outcomes for particular policy violations, establish priorities and strategies for enforcement, and describe how to escalate and respond to suspected violations. *See, e.g.,* **Exhibit L**, FB-CA-MAAG-NYAG-00037551 (a Platform enforcement rubric from 2018); **Exhibit M**, FB-CA-MAAG-NYAG-00019954 (enforcement rubric from 2012).[10]

32. Facebook has not asserted that any work product privilege or attorney client privilege attaches to these materials (and others like it) discussed in paragraphs 27-31.

33. Facebook has also claimed, in response to questions from members of the Senate Judiciary Committee, that in regular course of its business it engaged in "regular and proactive monitoring of apps" and "investigat[ing] for potential app violations":

> **[Q.] What is Facebook doing to monitor and investigate whether developers or others are taking and selling personal information?**
>
> [A.] .... We ... do a variety of manual and automated checks to ensure compliance with our policies and a positive experience for people. These include steps such as random checks of existing apps along with the regular and proactive monitoring of apps. We also respond to external or internal reports and investigate for potential app violations. When

[10] Exhibits L and M are dynamic Microsoft Excel spreadsheets produced by Facebook in their native format. To preserve the dynamic nature of the materials, Exhibits L and M are being filed with the Court on a CD in the same form as produced by Facebook (as native Microsoft Excel spreadsheets).

> we find evidence of or receive allegations of violations, we investigate and, where appropriate, employ a number of measures, including restricting applications from our platform, preventing developers from building on our platform in the future, and taking legal action where appropriate.
>
> * * *
>
> **[Q.] It is likely that there will not always be a newspaper reporting on every application developer that improperly sells user data. Has Facebook ever proactively (i.e., without being alerted by another party) learned about a similar violation of its terms of service - selling or transferring user data without consent to a third party - and if so, how? How many other such instances have you discovered?**
>
> [A]. We regularly take enforcement action against apps. For example, in 2017, we took action against about 370,000 apps, ranging from imposing certain restrictions to removal of the app from the platform.

Exhibit N at 121-22, 6.

Facebook's Failure to Detect and Prevent the Leak of User Data from the Platform

34. In or about 2013, a professor from the University of Cambridge, Professor Alexander Kogan, developed an app that he called "thisisyourdigitallife". Using the functionality of the Facebook Platform, Professor Kogan collected the personally-identifying data from the Facebook accounts of users who installed Kogan's App, as well as data from the accounts of each of their Facebook Friends. Such data included, as to individual users, name, birthdate, gender, language, age range, current city, a list of the names of all of the user's Friends, the Facebook pages the user had "liked," and for a smaller subset of users, email addresses, content of their Facebook posts, their Facebook messages, and photos. **Exhibit O** at FB-CA-AG-C001.009-10.

35. Ultimately, Professor Kogan obtained the personally-identifying data from the Facebook accounts of approximately 87 million Facebook users. He then sold some or all of that data to a political data analytics and advertising firm, Cambridge Analytica, and related entities Strategic Communication Laboratories ("SCL") and Eunoia Technologies, Inc. Professor

Kogan's sale of this data to Cambridge Analytica and related entities, according to Facebook, violated Facebook's Policies.

36. Despite its Platform Policies and various practices it claimed to have maintained to detect and prevent app developers from selling or transferring user data from the Platform or using it in ways not connected to the application, Facebook appears to have not detected Kogan's sale of data on its own. It discovered it only after being alerted to it in December 2015 through a media inquiry. *See* **Exhibit O** at FB-CA-AG-C001.015. In response, Facebook admitted that the sale of the data directly violated its Platform Policies, which "explicitly prohibited selling or licensing user data accessed from Facebook and from sharing any user data accessed from Facebook with any ad network, data broker, or other advertising or monetization-related service." *Id.* at FB-CA-AG-C001.003.

37. Facebook subsequently demanded that Kogan, Cambridge Analytica, and various affiliated third parties, delete the misappropriated data. **Exhibit P** at FB-AG-00000313; **Exhibit Q** at FB-AG-00000318. Facebook eventually obtained "certifications" from those parties that the data had been deleted. **Exhibit R** (SCL Elections Limited/ Alexander Nix, on behalf of Cambridge Analytica);[11] **Exhibit S** (GSR/Kogan), **Exhibit T** (Eunoia Technologies/Wylie).

38. In March 2018, media reports emerged claiming that Cambridge Analytica had not, contrary to its "certification" to Facebook, in fact, deleted the data it purchased from Kogan, but instead had used this consumer data without consumers' knowledge or consent to target consumers on Facebook with campaign messaging during the 2016 U.S. Presidential Election. **Exhibit U.**

[11] As SCL Elections limited is the company related to Cambridge Analytica that appears to have signed the agreement to purchase the Facebook data from GSR and/or Dr. Kogan, there does not appear to be an independent certification from Cambridge Analytica.

39. From December 2015 until March 2018, Facebook appears to have taken no other action against Cambridge Analytica or its affiliated entities aside from demanding that they delete the data and produce a "certification" of such destruction *(supra,* ¶ 37). Facebook did not shut off Cambridge Analytica's access to the Platform or other Facebook services, or its ability to take data from the Platform, or take any other steps to remedy the policy violation. Nor did it seek to disengage itself from any business dealings with Cambridge Analytica.

40. To the contrary, even as it was demanding in early January 2016 that Cambridge Analytica delete all user data it received from Professor Kogan in violation of its policies, it was accepting money from Cambridge Analytica as an advertiser on Facebook and courting its continued business. *See* **Exhibit V** (on January 12, 2016, Facebook emailed Cambridge Analytica's Chief Data Officer, Alex Tayler and demanded deletion of data as a condition of "maintain[ing] a positive relationship with" Facebook); **Exhibit W** (on January 15, 2016, Facebook advertising account representatives warned Cambridge Analytica that it was approaching its credit limit for advertising purchases and that "[i]t might be worth prepaying if you want to avoid going dark."); **Exhibit P** (on January 18, 2016, Cambridge Analytica's Chief Data Officer, Alex Tayler, confirmed to Facebook that had deleted data from Kogan); **Exhibit X** (on January 19, 2016, Facebook increased Cambridge Analytica's credit limit for advertising to $300,000); **Exhibit Y** at FB-CA-MAAG-NYAG-00015233 (on June 22, 2016, Cambridge Analytica employee reached out to Facebook wanting to "discuss CA and Facebook's overall relationship and how we can resolve some issues to maintain a better partnership"); **Exhibit Z** (on June 27, 2016, Facebook representatives emailed Cambridge Analytica employees: "[We are] excited to hear more about CA's growing business and how we can support your needs better!"); and **Exhibit AA** (On July 11, 2016, Cambridge Analytica employee thanked Facebook

for the "sweet box of swag" and expressed "[a]ppreciat[ion for] your continued help and partnership.").

41. Facebook also continued to allow Cambridge Analytica robust access to Facebook users for purposes of conducting advertising campaigns on behalf of its clients through 2016. *See* **Exhibit BB** at FB-CA-MAAG-NYAG-00016956 (discussing in late October 2016 an advertising test campaign to run "through election day," but that Facebook will only move forward with "as long as the budget/media weight is high enough [and] the creative is good"); **Exhibit CC** (a Cambridge Analytica employee thanking a Facebook employee in July 2016 for "walking through advertising strategies" with him and requested Cambridge Analytica be on a "whitelist" for additional data services provided by Facebook). Only once there was significant press attention in March of 2018 did Facebook finally shut off Cambridge Analytica's access to Facebook.

42. Other documents uncovered in the Attorney General's investigation suggest that, as the case of Cambridge Analytica illustrates, Facebook's decisions about how aggressively to enforce its policies against an app developer do not turn solely on the likelihood of harm to users. For example, Facebook's CEO, Mark Zuckerberg, shared to his senior team on November 19, 2012 that, on the Platform, "I'm assuming we enforce our policies against competitors much more strongly." **Exhibit DD** at FB-1155757[12] (highlight added). Additionally, Facebook employees considered in 2013 whether they should make advertising spending (internally known

[12] The Attorney General did not obtain Exhibit DD directly from Facebook, but rather from a collection of documents published publicly by the U.K.'s Department for Digital, Culture, Media & Sport on or about December 5, 2018. The Washington Post reported on the publication of these documents (and included in its report a link to the documents themselves, including Exhibit DD) on the same date. *See* Elizabeth Dwoskin, Craig Timberg, and Tony Romm, *Facebook Allegedly Offered Advertisers Special Access to Users' Data and Activities, According to Documents Released by British Lawmakers,* WASH. POST, December 5, 2018, *available at* https://www.washingtonpost.com/technology/2018/12/05/facebook-allegedly-offered-advertisers-special-access-users-data-activities-according-documents-released-by-british-lawmakers/.

as "NEKO") "a prerequisite for access to" permissions to access user data. **Exhibit EE** at FB-CA-MAAG-NYAG-00026484.

Facebook's Post-2018 Policy Enforcement and its "App Developer Investigation"

43. The media reports about Kogan's sale of Facebook user data to Cambridge Analytica generated widespread concern from the public, lawmakers, and regulators, including multiple U.S. Congressional committees and other international bodies, about Facebook's failure to prevent this misappropriation of user data from its Platform. Facebook responded to these news reports on March 21, 2018, via a blog post by its CEO, who stated that "[i]t is against our policies for developers to share data without people's consent" and that the episode was "a breach of trust between Kogan, Cambridge Analytica and Facebook" and "a breach of trust between Facebook and the people who share their data with us and expect us to protect it. We need to fix that." **Exhibit FF.**

44. Facebook further publicly admitted that this may not have been an isolated incident, that it had "seen abuse of our platform and the misuse of people's data, and we know we need to do more," and announced plans to take a variety of "important steps for the future of our platform." Among those steps was the "App Developer Investigation," or "ADI," which Facebook described as follows:

> We will investigate all apps that had access to large amounts of information before we changed our platform in 2014 to reduce data access, and we will conduct a full audit of any app with suspicious activity. If we find developers that misused personally identifiable information, we will ban them from our platform.

Exhibit GG.

45. Thereafter, in the months following its announcement of the ADI, Facebook updated the public about the ADI, claiming that it was "in full swing," and consisted of "two phases":

> First, a comprehensive review to identify every app that had access to this amount of Facebook data. And second, where we have concerns, we will conduct interviews, make requests for information (RFI) — which ask a series of detailed questions about the app and the data it has access to — and perform audits that may include on-site inspections.

Exhibit HH.

46. Facebook published on its website that it had "large teams of internal and external experts working hard to investigate these apps as quickly as possible," and that "[t]o date thousands of apps have been investigated and around 200 have been suspended — pending a thorough investigation into whether they did in fact misuse any data." *Id.*

47. Facebook further promoted the ADI as an effective response to the concerns of various members of Congress and Congressional Committees, which opened inquiries and hearings that focused on whether Facebook had adequately safeguarded user information. *See* **Exhibit II** at 3; **Exhibit JJ** at 2, 125, 128-129; **Exhibit N** at 8-11, 121-122.

48. At the same time that it announced its ADI, Facebook has acknowledged to its investors that an effective ADI could be inconsistent with maximizing the company's profits. In its April 26, 2018 quarterly SEC filing, Facebook admitted that the ADI presented significant financial and public relations risks to Facebook, to the extent it uncovered "additional incidents of misuse of user data or other undesirable activity by third parties," such as "the use of user data in a manner inconsistent with our terms or policies." Such discovery "may negatively affect user trust and engagement, harm our reputation and brands, and adversely affect our business and financial results," as well as "subject us to additional litigation and regulatory inquiries, which could subject us to monetary penalties and damages, divert management's time and attention, and lead to enhanced regulatory oversight." **Exhibit KK** at 46.

The AGO's Investigation

49. "General Laws c. 93A 'is a statute of broad impact' that prohibits 'unfair methods of competition' and 'unfair or deceptive acts or practices in the conduct of any trade or commerce.'" *Exxon Mobil Corp. v. Attorney Gen.,* 479 Mass. 312, 315-16 (2018), *cert. denied sub nom. Exxon Mobil Corp. v. Healey,* 139 S. Ct. 794 (2019), quoting *Slaney v. Westwood Auto. Inc,* 366 Mass. 688, 693-94 (1975).

50. The Attorney General has extensive authority under G.L. c. 93 A, § 6(1) to investigate entities that she believes have engaged or are engaging in any method, act or practice declared to be unlawful. *See Exxon Mobil,* 479 Mass at 324-25 (the Attorney General has "broad investigatory powers"); *CUNA Mut. Ins. Soc'y v. Attorney Gen.,* 380 Mass. 539, 542 n.5 (1980). This includes investigating the whether companies appropriately safeguard consumers' personal data from unauthorized use or disclosure, and whether they collect and use data consistently with consumers' informed consent, and not through deception or false pretenses. *See generally, Commonwealth v. Source One Assoc., Inc.,* 436 Mass. 118, 126 (2002); *see also,* G.L. c. 93H, §§ 2, 6.

51. Pursuant to her investigatory powers, the Attorney General may, through a civil investigative demand, "(a) take testimony under oath concerning such alleged unlawful method, act or practice; (b) examine or cause to be examined any documentary material of whatever nature relevant to such alleged unlawful method, act or practice; and (c) require attendance during such examination of documentary material of any person having knowledge of the documentary material and take testimony under oath or acknowledgment in respect of any such documentary material." G.L. c. 93A § 6(1).

52. Exercising this authority, the Attorney General opened an investigation into Facebook on or about March 20, 2018, following the media reports regarding the data exposure

to Cambridge Analytica, and in response to widespread concern about potential misuse of millions of Massachusetts' consumers' data dating back as far as 2012. Among other things, the Attorney General's investigation seeks to identify other instances of potential misuse and consumer harm, to assess whether Facebook has acted and is acting consistently with its representations to users regarding its policies and practices to safeguard their data on the Platform, and to identify other potential targets for investigation or enforcement action.

53. The Attorney General issued the first of three civil investigative demands to Facebook on April 23, 2018 (CID # 2018-CPD-25). During Facebook's production of materials to the first CID, Facebook informed the Attorney General that it had suspended (i.e. terminated the ability of the app to access user data from the Platform) 425 apps from the Platform as a result of an internal investigation. Facebook identified the apps and explained that they were associated with approximately six developers, but did not link each app to its developer, and did not disclose the basis for their suspension. *See* **Exhibit LL**; **Exhibit MM** at FB-CA-MAAG-NYAG-C009.03-C009.15.

54. In response, the Attorney General issued a second CID on June 20, 2018 (CID #2018-CPD-39). Therein, the Attorney General demanded that Facebook produce various identifying and factual information about the apps that it had suspended, including the identity of the app and its developer, whether the app was a test app or was released to the public, if and when Facebook had reviewed the app's privacy policy, the nature and amount of user data the app had permission to obtain, among other information. *See* **Exhibit NN** (Request 1). The Attorney General sought similar information with respect to apps that Facebook had undertaken to audit. *Id.* (Request 2).

55. The parties conferred regarding the second CID on or about July 5, 2018. Facebook requested that its responses to these demands be limited to the time period prior to its initiation of the ADI in or about March 30, 2018 and claimed that some of the requested materials were protected by the attorney work product doctrine. The Attorney General did not agree to this limitation and refused to withdraw the demands, but agreed to accept, as an initial matter, a narrative description of the ADI in an attempt to better understand the basis for the assertion of work product protection.

56. Facebook agreed, and provided a narrative description of the ADI to the Attorney General on August 13, 2018. Therein, Facebook described its then-current process as "constituted of two broad phases." **Exhibit OO** at FB-CA-MAAG-NYAG-C015.003. "Broadly speaking," Facebook explained, "the goal of the Phase One review is to identify apps whose developers may have engaged in misuse of Facebook user data." *Id.* at FB-CA-MAAG-NYAG-C015.004. "To assist in this process, Facebook's [DevOps] team is, at the direction of counsel, conducting a review of the apps for signals of potential misuse of user data[.]" *Id.* Facebook further explained:

> Through this review, the DevOps team examines information about an app, such as the developer's identity and associations; the app's past and present names; type of app; the app's URL; and available information about the app's historical usage. ...
> Facebook has prioritized for this review those apps that had the largest number of installations before Facebook changed its Graph API in 2014.
>
> ***
>
> If the Phase One review ... suggests that an app may have potentially engaged in misuse of Facebook user data, Facebook will escalate the app from Phase One to Phase Two ... [which involves a look] for signals that may suggest data misuse including those that may suggest sharing or selling of Facebook data—whether raw, aggregated, or derived—with or to third parties. This may also include signals of unauthorized or disproportionate data collection, broad data requests, storage of data longer than permitted under policy, and other related issues.

> In general, apps escalated to Phase Two undergo both a background investigation and a technical investigation. The goal of the combined investigation is to determine the likelihood that the app and/or developer violated Facebook policy, particularly related to potential data misuse.
>
> ***
>
> Based on the results of the background and technical investigations, Facebook will decide (i) if more information about an app and/or its developer is needed to determine risk of misuse of Facebook data; (ii) if some sort of enforcement action is recommended; or (iii) if no further action is needed.

Id.

Facebook's Refusal to Comply with Certain Demands in the CID

57. In an attempt to obtain information about other apps and developers that may have potentially misappropriated consumers' data from the Platform, and to assess whether Facebook has acted consistently with its representations in its Policies regarding its restriction of apps' collection, use, and disclosure of user data (or whether its enforcement of its Policies against app developers was influenced by financial or other considerations), the Attorney General issued its third CID—the CID at issue in this petition—on November 5, 2018 (CID #2018-CPD-67). **Exhibit A.**

58. As relevant to this Petition, the Attorney General demanded in the CID the following:

> 1. With respect to "Phase 1" of the Facebook App Developer investigation ("ADI"), as described in your August 13, 2018 letter describing Facebook's app developer investigation ("ADI") ("ADI Narrative") at FB-CA-MAAG-NYAG-C015.003-004[13], documents sufficient to identify each app reviewed in Phase 1 "that had access to large amounts of Facebook data before the 2014 changes to [its] Platform took effect" and each app "that c[a]me within the scope of the ADI review for other reasons, including through internal requests for investigative support or our Data Bounty program.[14]

[13] **Exhibit OO.**

[14] Facebook agreed to provide, and has been producing, documents responsive to a portion of Request 1, namely, the identities of those particular apps and app developers that came within the scope of the ADI from its Data Abuse Bug Bounty, which is program that Facebook implemented to field third-party referrals of apps that may have engaged in wrongful conduct.

In lieu of documents in response to this Request, the Commonwealth will accept information in a spreadsheet format.

2. As to each app identified in Request No. 1, documents sufficient to identify:

a. The app developer/publisher;

b. Whether the app was a test app or released to the public;

c. The date the app was first released to the public;

d. The date the app's privacy policy was first reviewed by You [(Facebook)], and a description of the nature of that review (e.g. manual review; confirmation of a URL, etc.);

e. The basis and initial source(s) of reports, allegations or concerns of data misuse of user information obtained or accessed through the app;

f. All categories of user information for which the app obtained permissions;

g. To date, the number of users who downloaded or installed the app; [and]

h. Number of users whose information was accessed or obtained by the app who did not download or install the app[.]

In lieu of documents in response to this Request, the Commonwealth will accept information in a spreadsheet format.

3. With respect to "Phase 2" of the ADI, as described at FB-CA-MAAG-NYAG-C015.003 and C015.004-005 of the ADI Narrative,[15] documents sufficient to identify:

a. Each app for which went to "Phase 2" for an "in-depth review";

b. Each app for which a "Background Information investigation" was conducted;

c. Each app for which a "Technical Investigation" was conducted;

d. Each app to which a request for information ("RFI") was sent;

e. Each app for which an interview was sought with the developer;

f. Each app for which a remote or onsite audit was requested to be conducted;

[15] **Exhibit OO.**

g. Each app for which "actual misuse" was identified, and documents sufficient to identify the "actual misuse";

h. Each app that was banned from the Platform for "actual misuse";

i. Each app that was banned from the Platform for "fail[ure] to cooperate with the investigation."

In lieu of documents in response to this Request, the Commonwealth will accept information in a spreadsheet format.

* * *

6. All internal communications and internal correspondence concerning the apps identified in response to Requests 1 [and] 3 ....

Exhibit A (the "Demands"). The Attorney General requested that Facebook respond to the Demands by November 20, 2018.

59. Facebook subsequently produced information responsive only to Demands 3(d)-(h). This information related to and identified those apps and developers with which Facebook has communicated with during the ADI, including through "Requests for Information," requests for an interview, or a demand for an audit. Facebook has also disclosed to the Attorney General the identity of various apps and developers, including by producing lists of approximately 69,000 apps associated with under 300 developers that it has suspended through its ADI.[16]

60. As to the remainder of Demands 1, 2, 3, and 6, Facebook has refused to comply. By letter dated December 4, 2018, Facebook refused to produce documents responsive to the Demands, asserting that the ADI was "conceived and run, from the beginning, by internal and external counsel ... in order to advice Facebook regarding its legal position and legal risk in

[16] Facebook has produced, and has seasonably updated, lists of the suspended apps. The vast majority of those suspensions were for the developer's failure to cooperate with Facebook's request for information. Because the lists are voluminous, a representative excerpt from the list provided on July 23, 2019 is attached hereto as **Exhibit PP**. Even this information as produced in a manner that unnecessarily complicates the Attorney General's investigation. For example, Facebook has separately provided the names of the developers associated with about 23,000 of the 69,000 apps, and even as to those, did not cross-reference each developer to its corresponding app(s) or provided any additional information that would allow this Office to discern which apps are associated with which developer. *See* **Exhibit QQ**.

relation to potential data misuse and activities by third-party app developers" and is "plainly a privileged effort." **Exhibit RR** at FB-CA-MAAG-NYA[G]-C018.02. Facebook has refused to comply with the Demands, claiming that they "call for the identification of apps reviewed at Phases 1 and 2 of [the ADI], and various data points associated with those apps, including the basis for their selection and review" and as such, "call[] for privileged selections and compilations of data. . . . Additionally, because the materials sought in Request 6 are internal communications undertaken at the direction of counsel, we do not have non-privileged materials responsive to that request." *Id.* at FB-CA-MAAG-NYA[G]-C018.04.

61. The Attorney General's Office responded by letter on December 24, 2018, disputing that the Demands sought information protected by the work product doctrine. **Exhibit SS.** The Attorney General's Office reiterated its Demands, noting that they sought purely factual information that could not reveal any protected thought processes of counsel—the names of apps and developers, dates of the app's release, dates that Facebook reviewed the app's privacy policy, categories of user information taken, and the number of users affected.

62. From December 2018 through June 2019, the parties engaged in numerous discussions by phone and in person to attempt to resolve, or narrow, any dispute. During those sessions and in related correspondence, Facebook provided additional information about the ADI, including high-level information as to how it prioritized apps for review, and other general investigative methods and processes.

63. Over the course of those discussions, Facebook has informed the Attorney General's Office that approximately 9 million apps, like the thisisyourdigitallife" app, had access to large amounts of information before Facebook reduced data access on the Platform in 2014 *(see supra* ¶¶ 44, 19, 20). It has also informed the Attorney General's Office that over the course

of the ADI, Facebook has identified approximately 2 million of those apps (associated with a much smaller number of developers) as warranting a closer examination for potential misuse of Facebook user data. Facebook has furthered narrowed this group into various, smaller subgroups of apps and developers with certain criteria that may suggest data misuse, including:

a. A group of 6,000 apps with a large number of installing users (and thus a potentially larger user impact with respect to potential data misuse) **Exhibit TT**; **Exhibit UU** at FB-CA-MAAG-C001.005;

b. A group of an unknown number of apps and developers that fall within certain categories that, based on Facebook's "past investigative experience," present elevated risk of potential policy violations. These categories include, for example, [redacted]." **Exhibit UU** at FB-CA-MAAG-C001.004;

c. A group of an unknown number of apps and developers that were reported to Facebook from outside of the ADI process, such as through the Data Abuse Bounty Program,[17] media reporting and inquiries, and other referrals from internal Facebook teams. *Id.* at FB-CA-MAAG-C001.005.

d. As of April 2019, a group of 2,000 apps and/or developers on which Facebook has conducted a "detailed background check ... to gauge whether the app or developer has engaged in behavior that may pose a risk to Facebook user data or raise suspicions of data misuse, to identify connections with other entities of interest, and to search for any other indications of fraudulent activity." *Id.* at FB-CA-MAAG-C001.006;

e. As of April 2019, a group of nearly 2,000 apps on which Facebook has conducted a "technical review" to analyze "available technical information about the apps derived from Facebook's available internal usage records in order to gauge data collection practices—such as the disproportionate collection of data and broad data requests—which may suggest data misuse." *Id.*

64. Facebook persists in refusing to identify any of the apps or developers within these more limited groups or any information about them, notwithstanding that such information falls squarely in the scope of the Attorney General Office's Demands.

[17] As noted *supra* n. 14, Facebook has identified those apps and developers that were brought to its attention through the Data Abuse Bounty Program.

This Court Should Compel Facebook's Compliance with the Demands

65. "A person upon whom a [CID] is served . . . shall comply with the terms thereof unless otherwise provided by the order of a court of the commonwealth. . . ." Gen. L. c. 93A, § 7. If the recipient fails to comply with the CID, the Attorney General's Office may petition the Superior Court to enforce compliance with the demand. *Id.*

66. A party that receives a CID may, "[a]t any time prior to the date specified in the notice, or within twenty-one days after the notice has been served" file a motion in the Superior Court to modify or set aside the demand. Gen. L. c. 93A, § 6(7). Facebook did not move to set aside or modify any of the CIDs issued by the Attorney General's Office, including the CID at issue in this Petition, prior to their return dates, or at any point.

67. The Attorney General has a substantial interest in identifying other instances of potential misuse of Facebook users' personal data, and in assessing whether Facebook has acted and is acting consistently with its representations to users regarding its policies and practices to safeguard their data on the Platform. The information Facebook is withholding about its investigation squarely informs these important questions by informing the Attorney General of the nature of Facebook's enforcement of its policy promises to consumers and whether Facebook has adequately safeguarded millions of consumers' data from unauthorized access and use by third parties, and, notwithstanding any such efforts, the identify of any third parties who obtained unauthorized access to or made unauthorized use of consumers' data and the scope, nature, and extent of any resulting consumer injuries.

68. Only Facebook knows the identity of the apps and developers that it has found may have engaged in suspicious behavior regarding consumers' data. There is no other source from which the Attorney General can obtain this data, and no other feasible method (i.e. depositions or interviews) to obtain this information.

69. As explained more fully in the accompanying Memorandum, information regarding third-party app developers who may have misappropriated consumers' Facebook data is not entitled to work product protection.

70. Facebook cannot establish good cause or otherwise meet its heavy burdens to avoid its obligation to comply fully with the CID, and has, in fact, waived any objection to the CIDs.

71. Facebook has necessitated this petition under G.L. c. 93A, § 7 by failing to comply fully or adequately with the CID, and withholding from the Attorney General facts that would identify other parties that may be misusing or misappropriating consumers' data, the scope of resulting harm, and other facts necessary to protect the public's interest and vindicate potential violations of c. 93A by Facebook and others.

[Remainder of this page intentionally left blank]

PRAYER FOR RELIEF

WHEREFORE, the Attorney General respectfully requests that this Honorable Court:

1. Grant the Attorney General's Petition to enforce CID No. 2018-CPD-67;

2. Order Facebook within 14 days of the Court's Order to comply in full with requests 1-3 and 6 in CID No. 2018-CPD-67, with respect to the following categories:

   a. That group of 6,000 apps with a large number of installing users, as referenced in **Exhibit TT** and **Exhibit UU** at FB-CA-MAAG-C001.005;

   b. That group of apps and developers that fall within certain categories that, based on Facebook's "past investigative experience," present elevated risk of potential policy violations, as referenced at **Exhibit UU** at FB-CA-MAAG-C001.004;

   c. That group of apps and developers that were reported to Facebook from outside of the ADI process, such as through the Data Abuse Bounty Program (to the extent not already produced), media reporting and inquiries, and other referrals from internal Facebook teams, as referenced in **Exhibit UU** at FB-CA-MAAG-C001.004;

   d. That group of apps and/or developers on which, to date, Facebook has conducted a "detailed background check ... to gauge whether the app or developer has engaged in behavior that may pose a risk to Facebook user data or raise suspicions of data misuse, to identify connections with other entities of interest, and to search for any other indications of fraudulent activity," as referenced in **Exhibit UU** at FB-CA-MAAG-C001.006; and

   e. That group of apps on which, to date, Facebook has conducted a "technical review" to analyze "available technical information about the apps derived from Facebook's available internal usage records in order to gauge data collection practices—such as the disproportionate collection of data and broad data requests—which may suggest data misuse," as referenced in **Exhibit UU** at FB-CA-MAAG-C001.006; and

3. Order such other relief as the Court deems just and appropriate.

Respectfully submitted,
MAURA HEALEY
Attorney General of the
Commonwealth of Massachusetts

_____
Sara Cable, BBO # 667084

Assistant Attorney General,
Director, Data Privacy & Security Unit

Jared Rinehimer, BBO # 684701
Assistant Attorney General

Peter Downing, BBO # 675969
Assistant Attorney General

Consumer Protection Division
Office of Attorney General Maura Healey
One Ashburton Place
Boston, MA 02108
(617) 727-2200
sara.cable@mass.gov
jared.rinehimer@mass.gov
peter.dovming@mass.gov

Dated: August 15, 2019

Certificate of Service

I, Sara Cable, hereby certify that a true copy of the above document was served upon the following on _____

By certified mail, return receipt requested:

Facebook, Inc.
1 Hacker Way (1601 Willow Road),
Menlo Park, California 94025

Facebook, Inc.
c/o Corporation Service Company
84 State Street
Boston, MA 02109.

By certified mail, return receipt requested, and e-mail:

Facebook, Inc.
c/o Anjan Sahni, Esq.
WilmerHale
7 World Trade Center
250 Greenwich St.
New York, NY 10007.

_____
Sara Cable

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT
CIVIL ACTION NO.

ATTORNEY GENERAL
MAURA HEALEY,

Petitioner,

v.

FACEBOOK, INC.,

Respondent.

EXHIBIT INDEX

TO ATTORNEY GENERAL'S PETITION TO COMPEL COMPLIANCE WITH CIVIL INVESTIGATIVE DEMAND PURSUANT TO G.L. C. 93A, § 7

Exhibit	Description
A	Civil Investigative Demand No. 2018-CPD-67, dated November 5, 2018
B	Excerpts of Facebook's Amendment No. 4 to Form S-1, Registration Statement, filed on April 23, 2012 with the U.S. Securities & Exchange Commission
C	Facebook, *The New Facebook Login and Graph API 2.0,* "News for Developers," April 30, 2014, https://developers.facebook.com/blog/post/2014/04/30/the-new-facebook-login (last visited 8/12/19)
D	Facebook's Statement of Rights and Responsibilities as of Dec. 11, 2012
E	Facebook's Platform Policies as of Feb. 20, 2013
F	Facebook's Platform Policies as of July 24, 2014
G	Facebook's Data Use Policy as of Dec. 11, 2012
H	Facebook's Data Use Policy as of Nov. 15, 2013
I	Letter from A. Sahni to S. Cable, dated July 20, 2018 (bates numbered FB-CA-MAAG-NYAG-C012.01-C012.18)
J	Document produced by Facebook under bates number FB-CA-MAAG-NYAG-00037557

K	Document produced by Facebook under bates number FB-CA-MAAG-NYAG-00041067
L	Document produced by Facebook under bates number FB-CA-MAAG-NYAG-00037551 (filed on CD only)
M	Document produced by Facebook under bates number FB-CA-MAAG-NYAG-00019954 (filed on CD only)
N	Excerpts from Facebook's answers to Questions for the Record from U.S. Senators Coons and Feinstein, following an April 10, 2018 Hearing before the U.S. Senate Committee on the Judiciary, titled "Facebook, Social Media Privacy, and the Use and Abuse of Data," dated June 8, 2018
O	Excerpts from April 13, 2018 letter from Facebook to various Attorneys General
P	Document produced by Facebook under bates number FB-00000313
Q	Document produced by Facebook under bates number FB-00000318
R	Document produced by Facebook under bates number FB-00000359
S	Document produced by Facebook under bates number FB-00001105
T	Document produced by Facebook under bates number FB-00001097
U	Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions,* N.Y. TIMES (published on March 17, 2018), *available at* https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html
V	Document produced by Facebook under bates number FB-CA-MAAG-NYAG-00012526
W	Document produced by Facebook under bates number FB-CA-MAAG-NYAG-00012547
X	Document produced by Facebook under bates number FB-CA-MAAG-NYAG-00012576
Y	Document produced by Facebook under bates number FB-CA-MAAG-NYAG-00015232
Z	Document produced by Facebook under bates number FB-CA-MAAG-NYAG-00015271

AA	Document produced by Facebook under bates number FB-CA-MAAG-NYAG-00015805
BB	Document produced by Facebook under bates number FB-CA-MAAG-NYAG-00016956
CC	Document produced by Facebook under bates number FB-CA-MAAG-NYAG-00015386
DD	Excerpts from documents published publicly on or about December 5, 2018 by the U.K.'s Department for Digital, Culture, Media and Sport
EE	Document produced by Facebook under bates number FB-CA-MAAG-NYAG-00026480
FF	Facebook, statement by Mark Zuckerberg, posted on March 21, 2018 at https://www.facebook.com/zuck/posts/10104712037900071
GG	Facebook, *Cracking Down on Platform Abuse*, Facebook's Newsroom, March 21, 2018, https://newsroom.fb.com/news/2018/03/cracking-down-on-platform-abuse/(last visited 8/12/19)
HH	Facebook, *An Update on Our App Investigation and Audit,* May 14, 2018, https://newsroom.fb.com/news/2018/05/update-on-app-audit/ (last visited 8/12/19)
II	Written testimony of Mark Zuckerberg at a hearing before the U.S. House of Representatives, Committee on Energy and Commerce on April 11, 2018
JJ	Excerpts from Facebook's answers to Questions for the Record from U.S. Senators Thune and Blumenthal, following an April 10, 2018 Hearing before the U.S. Senate Committee on Commerce, Science, and Transportation, titled "Facebook, Social Media Privacy, and the Use and Abuse of Data," dated June 8, 2018
KK	Excerpts from Facebook's 10-Q filing with the U.S. Securities & Exchange Commission, dated April 26, 2018
LL	Letter from B. Powell to S. Cable, dated May 29, 2018 (bates numbered FB-CA-MAAG-NYAG-C007.01-C007.09)
MM	Letter from B. Powell to S. Cable, dated June 12, 2018 (bates numbered FB-CA-MAAG-NYAG-C009.01-C009.15)
NN	Civil Investigative Demand No. CID #2018-CPD-39, dated June 20, 2018
OO	Letter from A. Sahni to S. Cable, dated August 13, 2018 (bates numbered FB-CA-MAAG-NYAG-C015.01-C015.06)

PP	Excerpts from Letter from A. Sahni to S. Cable, dated July 23, 2019 (bates numbered FB-CA-MAAG-NYAG-C038.0001-C038.1053)
QQ	Letter from A. Sahni to S. Cable, dated May 10, 2019 (bates numbered FB-CA-MAAG-NYAG-C035.001-C035.008)
RR	Letter from A. Sahni to S. Cable, dated December 4, 2018 (bates numbered FB-CA-MAAG-NYAG-C018.01-C018.07)
SS	Letter from S. Cable to A. Sahni, dated December 24, 2018
TT	E-mail from A. Sahni to J. Rinehimer and others, dated June 12, 2019
UU	Letter from A. Sahni to S. Cable, dated July 1, 2019 (bates numbered FB-CA-MAAG-C001.002-C001.008)